SECURITY INTELLIGENCE GOES MOBILE

Keeping Your Organization Safe Wherever You Go

KASPERSKY lab

Whether a business has an IT department of 1 or 100, an official BYOD policy, or just employees or clients with mobile devices (in other words, employees and clients), mobile malware matters to your organization… or it should. It's imperative that you consider the security risks beyond your PCs and servers.

Keeping up with viruses and cybercrime on mobile devices is even more difficult than keeping up with the latest mobile technology. In the first quarter of 2014, the percentage of threats targeting Android™ exceeded 99% of all mobile malware, including:

- 1,258,436 installation packages
- 110,324 new malicious programs for mobile devices
- 1,182 new mobile banking Trojans

Is your organization keeping up with mobile cyberthreats? It's important to partner with cybersecurity experts you can trust to keep your organization out of harm's way. This eBook contains information about the latest mobile threats, including Faketoken, Tor-controlled bots, eWallet thefts, malicious spam, and other mobile malware.

Faketoken

Faketoken is a banking Trojan that entered Kaspersky Lab's Top 20 most frequently detected threats by the end of the quarter. This mobile threat steals mTANs and works in concert with computer-based banking Trojans. During an online banking session, the computer-based Trojans use a web inject to seed a request on the infected webpage to download an Android application that is allegedly needed in order to conduct secure transactions, but the link actually leads to Faketoken. After the mobile threat ends up on a user's smartphone, cybercriminals then use the computer-based Trojans to gain access to the victim's bank account, and Faketoken allows them to harvest mTANs and transfer the victim's money to their accounts.

During the first three months of 2014, Kaspersky Lab detected attacks involving this threat in 55 countries, including Germany, Sweden, France, Italy, the UK, and the US.

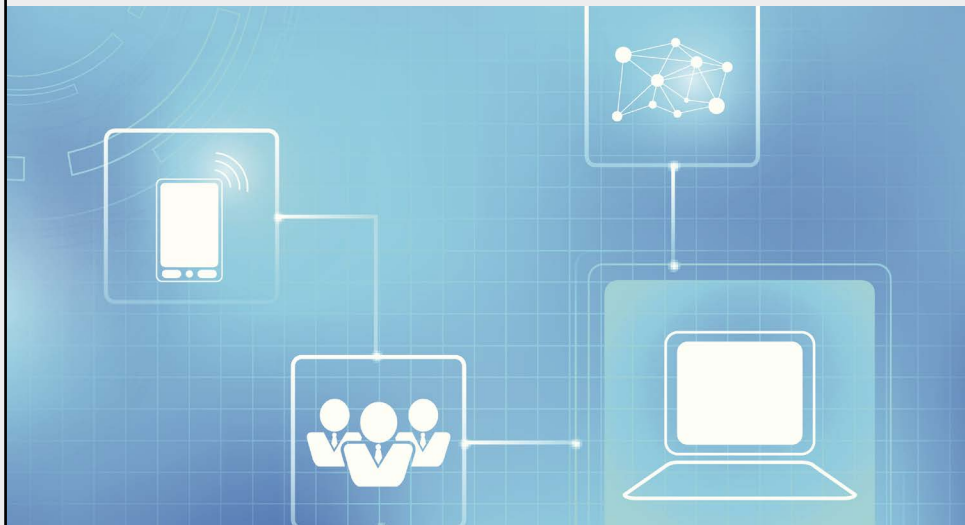
Tor-Controlled Bots

The anonymous Tor network, which is built on a network of proxy servers, offers user anonymity and allows participants to host “anonymous” websites on the .onion domain zone. These websites are then only accessible through Tor. In February, Kaspersky Lab detected the first Android Trojan that is run through a C&C hosted on a domain in the .onion pseudo-zone. Backdoor.AndroidOS.Torec.a is a modification of Orbot, a commonly used Tor client, in which malicious users have seeded their own code. Note that in order to ensure that Backdoor.AndroidOS.Torec.a is able to use Tor, it needs much more code than for its main function.

This Trojan can receive the following commands from the C&C:

- Initiate / stop the interception of incoming text messages
- Initiate / stop the theft of incoming text messages
- Issue a USSD request
- Send data about a telephone (the phone number, country, IMEI, model, OS version) to the C&C
- Send a list of apps installed on a mobile device to the C&C
- Send text messages to a number specified in a command

Why did malicious users find there was a need for an anonymous network? The answer is simple: a C&C hosted on the Tor network cannot be shut down. Incidentally, the creators of Android Trojans adapted this approach from the virus writers who developed threats targeting Windows®.



E-Wallet Thefts

Malicious users are always on the lookout for new ways to steal money using mobile Trojans. In March, Kaspersky Lab detected Trojan-SMS.AndroidOS.Waller.a, which in addition to typical SMS Trojan functions is also capable of stealing money from QIWI wallets on infected phones.

Once it receives the appropriate C&C command, the Trojan checks the QIWI wallet balance by sending a text message to the corresponding QIWI system number. The Trojan intercepts the response and sends it to its operators.

If the owner of the infected device has a QIWI wallet account and the Trojan obtains data that there is a positive balance in the wallet account, the malware can transfer money from the user's account to the QIWI wallet account specified by the cybercriminals. The Trojan owners send a special QIWI system number by text indicating the wallet ID of the malicious users, and the amount to be transferred. So far, this Trojan has only targeted Russian users. However, cybercriminals can use it to steal cash from users in other countries where text-managed e-wallet systems are commonly used.

Malicious Spam

One of the standard methods used to spread mobile malware is malicious spam. This method is one of the top choices among cybercriminals who use mobile Trojans to steal money from user bank accounts. Malicious spam texts typically contain either an offer to download an app using a link that points to malware, or a link to a website seeded with a malicious program that redirects users to some sort of offer. Just like with malicious spam in email, cybercriminals rely heavily on social engineering to get the user's attention.

Spam with Links To Malicious Websites

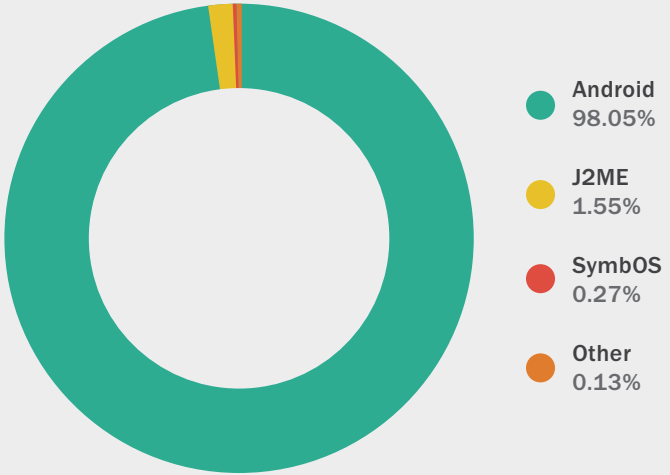
The cybercriminals who spread the Opfake Trojan sent out SMS spam with a link to specially created malicious websites. One of the text messages informed recipients that they had received a package and led to a website disguised as the Russian Postal Service.

2013 in Figures

- A total of 143,211 new modifications of malicious programs targeting mobile devices were detected in all of 2013 (as of January 1, 2014).
- In 2013, 3,905,502 installation packages were used by cybercriminals to distribute mobile malware. Overall in 2012-2013 we detected approximately 10,000,000 unique malicious installation packages.
- Different installation packages can install programs with the same functionality that differ only in terms of the malicious app interface and the content of the text messages it spreads.

The Distribution of Mobile Malware by Platform

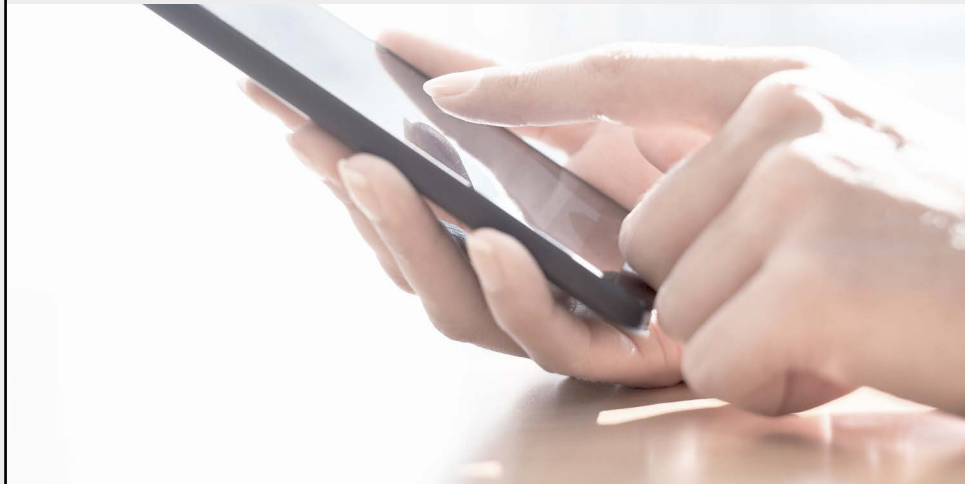
Android remains a prime target for malicious attacks. 98.05% of all malware detected in 2013 targeted this platform, confirming both the popularity of this mobile OS and the vulnerability of its architecture.



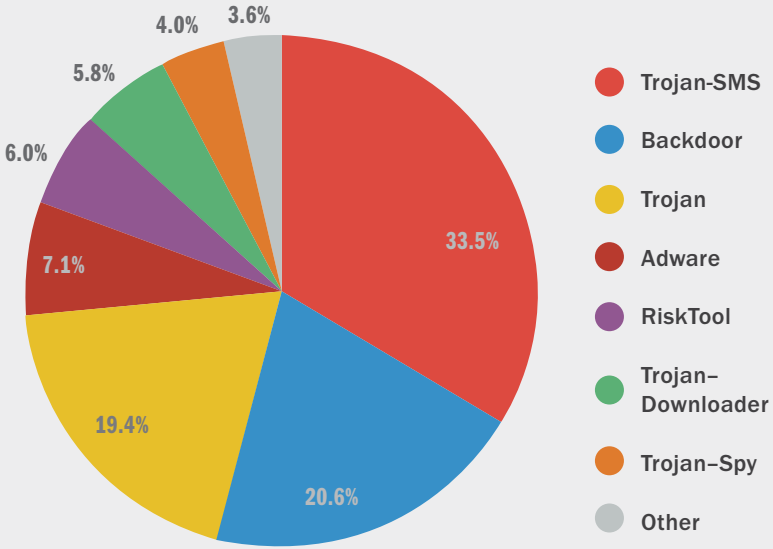
Android's obvious vulnerability doesn't mean all other platforms are safe, however. In the first quarter of 2014, a Trojan targeting iOS was detected. This malicious program is a plug-in for Cydia Substrate, a widely used framework for rooted/hacked devices. There are many affiliate programs for app developers allowing them to promote their apps using the advertising module, and earn money for ad displays. In some advertising modules, the Trojan switches out the ID of the app developers for the malicious users' ID. As a result, all of the money for ad displays goes to the malicious users instead.

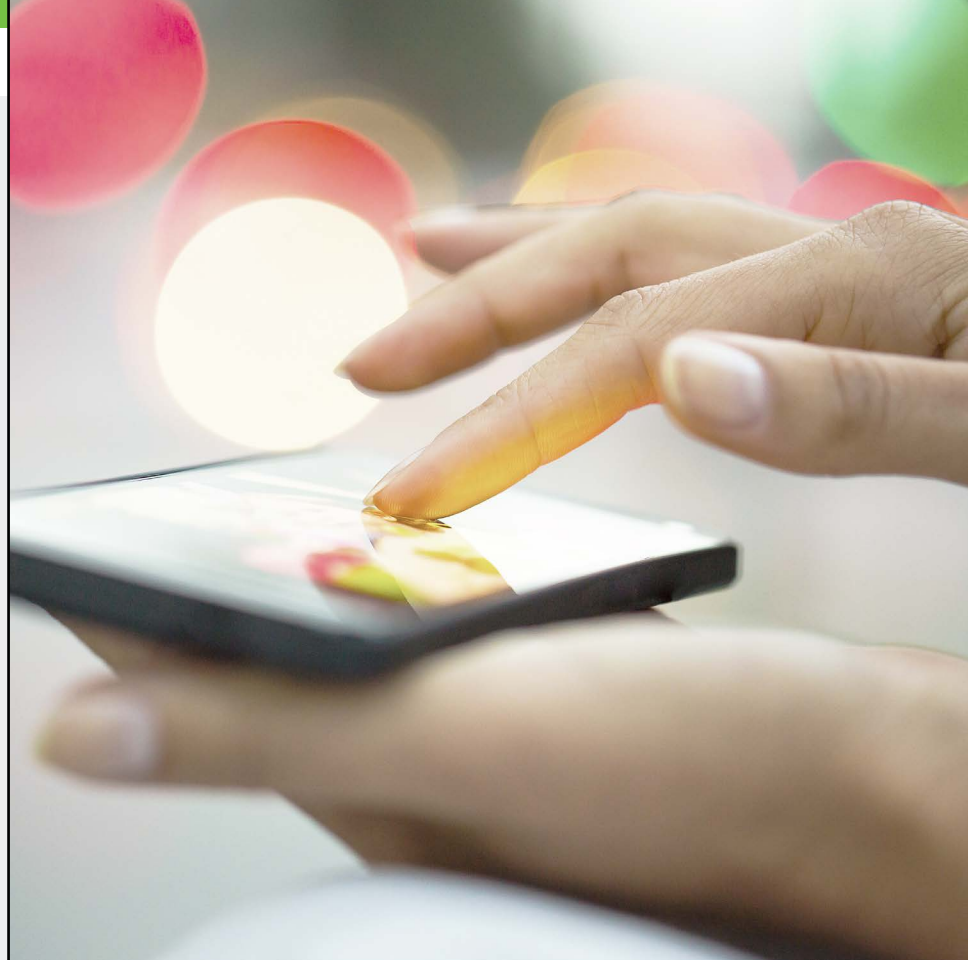
Experts from Turkey have detected a vulnerability exploit causing a denial of service on a device and a subsequent reboot. The point of this vulnerability is that malicious users can take advantage of it to develop an Android app with AndroidManifest.xml, which contains a large amount of data in any name field (AndroidManfiest.xml is a special file found in every Android app). This file contains data about the app, including access permissions for system functions, markers for the processors for different events, etc. A new app can be installed without any issues but, for example, when an activity is called up with a specific name, the device will crash.

For instance, a handler can be developed for incoming text messages using the wrong name, and after receiving any text message, the phone would simply crash and become unusable. The device will start to continually reboot, and the user will have only one way of resolving the problem: rolling back the firmware, which will lead to the loss of all of the data stored on the device.



The Distribution of Mobile Malware by Category





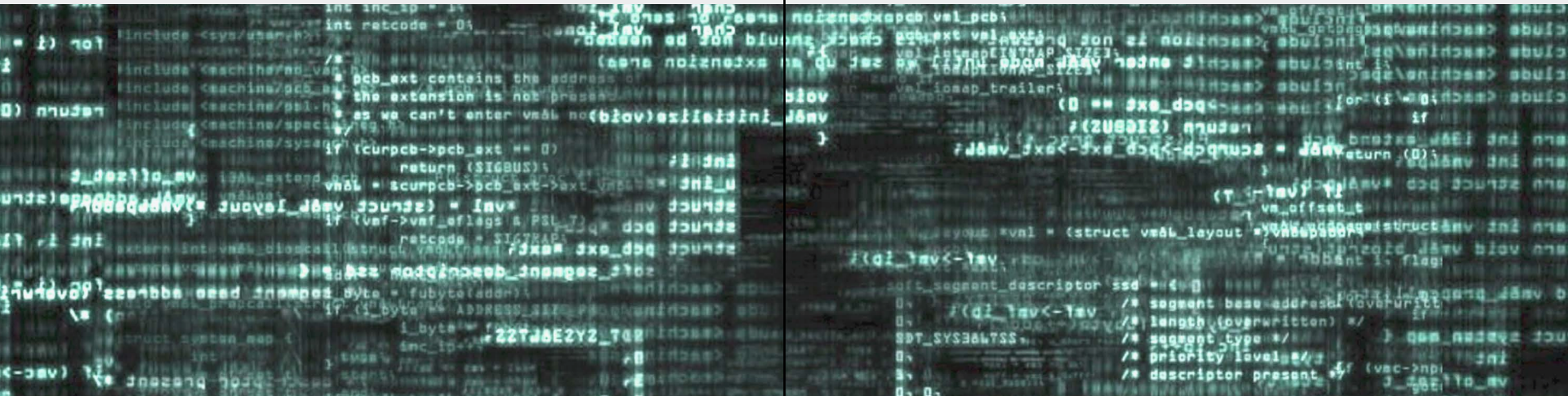
Methods and techniques

2013 saw a radical increase in output from mobile virus writers as well as the prevalence of applying methods and technologies that allowed cybercriminals to use their malware more effectively. There were several distinct areas where mobile malware underwent advances.

Distribution

Cybercriminals made use of some exceptionally sophisticated methods to infect mobile devices, including:

- Infecting legal web resources
- Distribution via alternative app stores
- Distribution via botnets



Resistance to anti-malware protection

The ability of malicious software to operate continuously on the victim's mobile device is an important aspect of its development. The longer a Trojan "lives" on a smartphone, the more money it will make for the owner. This is an area where virus writers are actively working, resulting in a large number of technological innovations.

Criminals are increasingly using obfuscation, the deliberate act of creating complex code to make it difficult to analyze. The more complex the obfuscation, the longer it will take an antivirus solution to neutralize the malicious code. Tellingly, current virus writers have mastered commercial obfuscators. This implies they have made considerable investments. For example, one commercial obfuscator, which cost €350, was used for Trojans and Opfak.bo Obad.a.

Android vulnerabilities are used by criminals for three main reasons: to bypass the code integrity check when installing an application (vulnerability Master Key); to enhance the rights of malicious applications, considerably extending their capabilities; and to make it more difficult to remove malware. For example, Svpeng uses a previously unknown vulnerability to protect itself from being removed manually or by the antivirus program.

Cybercriminals also exploit the Master Key vulnerability and have learned to embed unsigned executable files in Android installation packages. Digital signature verification can be bypassed by giving the malicious file exactly the same name as a legitimate file and placing it on the same level in the archive. The system verifies the signature of the legitimate file while installing the malicious file.

Unfortunately, there is a specific feature of Android vulnerabilities that means it is only possible to get rid of them by receiving an update from the device manufacturers. However, many users are in no hurry to update the operating systems of their products. If a smartphone or tablet was released more than a year ago, it is probably no longer supported by the manufacturer and patching of vulnerabilities is no longer provided. In that case, the only help comes from an antivirus solution, for example, Kaspersky Internet Security for Android.

Embedding malicious code in legitimate programs helps conceal infections from the victim. Of course, this does not mean the digital signature of the software developer can be used. However, due to the absence of certification centers verifying the digital signatures of Android programs, nothing prevents criminals from adding their own signature. As a result, a copy of Angry Birds installed from an unofficial app store or downloaded from a forum could easily contain malicious functionality.

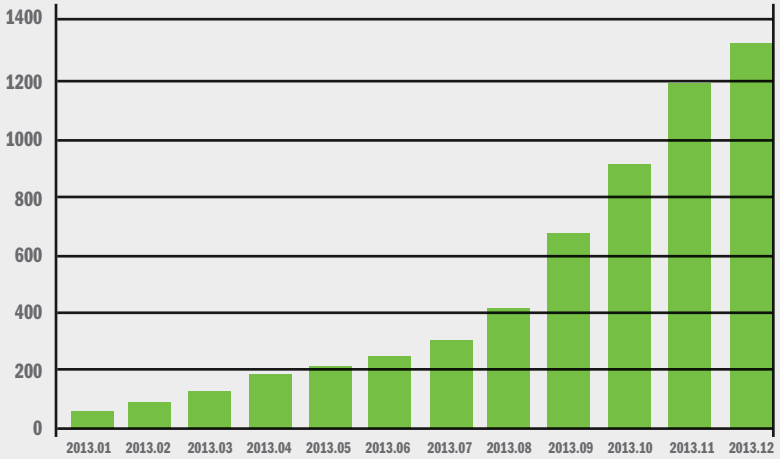
Capabilities and functionality

In 2013, Kaspersky Security Network detected several technological innovations developed and used by criminals in their malicious software, including:

- Control of malware from a single center provides maximum flexibility
- By using Google Cloud Messaging
- Attacks on Windows XP

The most advanced malicious mobile programs today are Trojans targeting users' bank accounts – the most attractive source of criminal earnings. 2013 was marked by a rapid rise in the number of Android banking Trojans. The cyberindustry of mobile malware is becoming more focused on making profits more effectively (i.e., mobile phishing, theft of credit card information, money transfers from bank cards to mobile phones and from phones to the criminals' e-wallets). Cybercriminals have become obsessed by this method of illegal earnings: at the beginning of the year we knew only 67 banking Trojans, but by the end of the year there were already 1321 unique samples. Kaspersky Lab mobile products prevented 2,500 infections by banking Trojans.

THE NUMBER OF MOBILE BANKING TROJANS IN OUR COLLECTION



Mobile banking Trojans can run together with Win-32 Trojans to bypass the two-factor authentication – mTAN theft (the theft of banking verification codes that banks send their customers in SMS messages). However, in 2013, autonomous mobile banking Trojans developed further. Currently, such Trojans attack a limited number of bank customers, but it is expected that cybercriminals will invent new techniques that will allow them to expand the number and the geography of potential victims. Today, the majority of banking Trojan attacks affects users in Russia and the CIS. However, this situation will not last long: given the cybercriminals' interest in user bank accounts, the activity of mobile banking Trojans is expected to grow in other countries in 2014. Banking Trojans are perhaps the most complex of all mobile threats, and Svpeng is one of the most striking examples.

Svpeng

In mid-July, the Kaspersky Security Network detected Trojan-SMS.AndroidOS.Svpeng.a. Unlike, its SMS Trojan counterparts, is focused on stealing money from the victim's bank account rather than from his mobile phone. It cannot act independently and operates strictly in accordance with commands received from the C&C server. This malicious program spreads via SMS spam and from compromised legitimate sites that redirect mobile users to a malicious resource. There the user is prompted to download and install a Trojan imitating an Adobe Flash Player® update.

Svpeng is capable of wreaking some serious havoc via an infected mobile device:

- It collects information about the smartphone.
- It steals SMS messages and information about voice calls.
- It steals money from the victim's bank account.
- It steals logins and passwords to online banking accounts.
- It steals bank card information.
- It extorts money from users by threatening to block the smartphone.
- It hides traces of its activity.
- It protects itself from deletion.

The Trojan is distributed in Russia and CIS countries. But, as we have already mentioned, the criminals could easily turn their attention to users in other countries.

Top 5 families of mobile malware distributed in the US

Family	# of All Attacked Unique Users
DangerousObject.Multi.Generic	19.75%
RiskTool.AndroidOS.SMSreg	19.24%
Monitor.AndroidOS.Walien	11.24%
Backdoor.AndroidOS.GinMaster	8.05%
AdWare.AndroidOS.Ganlet	7.29%

Malicious software that attacks users of mobile banking accounts continues to develop and the number of programs is growing rapidly. It is obvious that this trend will continue, with more mobile banking Trojans and new technologies to avoid detection and removal.

Of all the mobile malware samples detected in 2013, bots were the most populated category. The attackers have clearly seen the benefits of mobile botnets when it comes to making profits. New mechanisms for controlling mobile botnets may appear in the near future. In 2014 we expect to see vulnerabilities of all types being actively exploited to give malware root access on devices, making removal even more difficult.

2013 saw the first registered malware attack on a PC launched from a mobile device. We forecast future Wi-Fi attacks from mobile devices on neighboring workstations and the wider infrastructure. SMS Trojans are likely to remain among the mobile malware leaders and even conquer new territories.

Trusting the Mobile Security Experts

Kaspersky Lab keeps track of relevant mobile malware data for our customers and creates security solutions to protect their devices against the threats of today and tomorrow. At the start of 2014, Kaspersky Lab had logged 1,321 unique executables for mobile banking Trojans, and by the end of the first quarter, that number jumped to 2,503[1]. Most mobile malware is designed to steal users' money, including SMS-Trojans, and lots of backdoors and Trojans.

According to KSN data, Kaspersky Lab's products are making a difference in the impact of mobile malware[2]:

- Kaspersky Lab products blocked a total of 1,131,000,866 malicious attacks on computers and mobile devices in the first quarter of 2014.
- Kaspersky Lab solutions repelled 353,216,351 attacks launched from online resources located all over the world.
- Kaspersky Lab's web antivirus detected 29,122,849 unique malicious objects (e.g., scripts, web pages, exploits, executable files, etc.)
- 81,736,783 unique URLs were recognized as malicious by web antivirus.
- In 2013, Kaspersky Lab mobile products prevented 2,500 infections by banking Trojans[3].
- Over the year, the number of mobile malware modifications designed for phishing to steal credit card information and money increased by a factor of 19.7.
- 39% of web attacks neutralized by Kaspersky Lab products were carried out using malicious web resources located in the US and Russia.
- Kaspersky Lab's antivirus solutions detected 645,809,230 virus attacks on users' computers.
- A total of 135,227,372 unique malicious and potentially unwanted objects were identified in these incidents.

1 IT Threat Evolution Q1 2014, Emm, Chebyshev, Unuchek, and Garnaeva, May 2014.
2 IT Threat Evolution Q1 2014, Emm, Chebyshev, Unuchek, and Garnaeva, May 2014.
3 February 2014, SecureList, Mobile Malware Evolution: 2013

About Kaspersky Lab

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users*. Throughout its more than 16-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. With its holding company registered in the United Kingdom, Kaspersky Lab operates in almost 200 countries and territories worldwide, providing protection for over 300 million users worldwide.

Call Kaspersky today at 866-563-3099 or email us at corporatesales@kaspersky.com, to learn more about Kaspersky Endpoint Security for Business.

www.kaspersky.com/business

*The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC # 242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.